IMPLEMENTASI RSA ALGORITHM DAN CYRPTOGRAPHY QUANTUM PADA SISTEM LOGIN

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

Teknik Informatika Universitas Muhammadiyah Malang

Oleh :

Ridwan Annas pryagung

201510370311077

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2019

LEMBAR PERSETUJUAN

IMPLEMENTASI RSA ALGORITHM DAN CYRPTOGRAPHY QUANTUM PADA SISTEM LOGIN

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana Strata 1
Teknik Informatika Universitas Muhammadiyah Malang

Ridwan Annas Pryagung
201510370311077

Menyetujui,

Dosen I	Dosen II
Aminudin, S.Kom, M.Cs	**Sofyan Arifianto, S.Si, M.Kom**
NIDN. 0701068603	**NIDN. 0721058309**

i

LEMBAR PENGESAHAN

IMPLEMENTASI RSA ALGORITHM DAN CYRPTOGRAPHY QUANTUM PADA SISTEM LOGIN

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana Strata 1
Teknik Informatika Universitas Muhammadiyah Malang

Ridwan Annas Pryagung
201510370311077

Menyetujui,

Penguji I	Penguji II
Didih Rizki S.kom, M.kom	**Wildan Suharso S.kom, M.kom**
NIDN. 0702109201	**NIDN. 0730038405**

Mengetahui
Ketua Program Studi Teknik Informatika

Gita Indah Marthasari, ST., M.Kom.
NIDN. 720038101

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	: Ridwan Annas pryagung
Tempat, Tanggal Lahir	: Kediri, 07 april 1996
NIM	: 201510370311077
Fakultas/ Jurusan	: Teknik/ Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul "IMPLEMENTASI RSA ALGORITHM DAN CYRPTOGRAPHY QUANTUM PADA SISTEM LOGIN" beserta isinya adalah karya penulis sendiri dan bukan merupakan karya tulisan orang lain, baik sebagian atau seluruhnya, kecuali bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dala karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko atau sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Aminudin, S.Kom, M.Cs
NIDN. 0701068603

Malang, 30 September 2019

Ridwan Annas Pryagung
NIM. 201510370311077

KATA PENGANTAR

Puji syukur kehadirat Allah Subhanahu Wa Ta'ala atas limpahan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul Implementasi RSA Algorithm dan Cyrptography Quantum pada Sistem Login. Tulisan ini disajikan pokok-pokok bahasan mengenai algoritma RSA standar, improvisasi RSA, dan Quantum kriptografi mulai cara kerja, performa waktu, celah keamanan hingga pengembangannya. Selain itu juga dijelaskan mengenai pengaplikasian, pengujian waktu serta pengujian keamanan algoritma RSA standar, improvisasi RSA, dan Quantum Kriptografi. Peneliti menyadari sepenuhnya bahwa dalam penulisan tugas akhir ini masih banyak kekurangan dan keterbatasan. Oleh karena itu, peneliti sangat mengharapkan saran yang membangun agar tulisan ini bermanfaat untuk perkembangan ilmu pengetahuan kedepan.

Malang, 30 September 2019

Penulis

Ridwan Annas Pryagung

DAFTAR ISI

Daftar Gambar

Daftar Tabel

Daftar Lampiran

DAFTAR PUSTAKA

[1] Paryati, “Keamanan SIM,” vol. 2008, no. semnasIF, pp. 379–386, 2008.

[2] A. D. Laksono and S. Kom, “Keamanan Sistem Komputer,” pp. 1–11, 2017.

[3] D. Ganguly and S. Lahiri, *Cryptography and Network Security*. 2012.

[4] M. Bhavsingh, M. S. Lakshmi, S. P. Kumar, and N. Parashuram, “Improved Trial Division Algorithm by Lagrange ‟ s Interpolation Function,” no. May, pp. 1227–1231, 2017.

[5] P. Pajic, “Quantum Cryptography,” pp. 1–6, 2013.

[6] B. S. Muchlis, M. A. Budiman, and D. Rachmawati, “Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik,” *SinkrOn*, vol. 2, no. 2, pp. 49–64, 2017.

[7] K. Anggit, “The implementation of Asymmetric Algorithms Dual Modulus RSA in Applications Chat.” pp. 1–9, 2018.

[8] J. Informatika, F. Teknik, and U. M. Malang, “Analisa Hybrid Kriptosistem RSA dan EL-GAMAL pada Instant Messaging berbasis socket TCP,” no. 09560491, 2018.

[9] L. Ming-xin and K. Feng, “IJ " I Ja I,” no. Iccasm, pp. 35–37, 2010.

[10] K. Somsuk, “Higher Security for Login System Using RSA and One-time Pad Schemes,” vol. 10, no. 1, pp. 99–103, 2018.

[11] M. Ihwani, “Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma Rsa,” *CESSJournal Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 15–20, 2016.

[12] E. R. Sardju, R. Magdalena, and R. D. Atmaja, “Implementasi Algoritma Rsa Untuk Enkripsi Dan Dekripsi Sms (short Message Service) Pada Ponsel Berbasis Android,” *eProceedings Eng.*, vol. 2, no. 2, pp. 2435–2442, 2015.

[13] D. Wulansari, “Implementation of RSA Algorithm with Chinese Remainder Theorem for Modulus N 1024 Bit and 4096 Bit,” no. 10, pp. 186–194.

[14] N. Somani and D. Mangal, “An Improved RSA Cryptographic System,” *Int. J. Comput. Appl.*, vol. 105, no. 16, pp. 975–8887, 2014.

[15] S. Kromodimoeljo, *Teori&aplikasi kriptografi*. SPK IT Consulting.

[16] H. R. Sandityas, “Analisa Hybrid Kriptosistem RSA dan EL-GAMAL pada Instant Messaging berbasis socket TCP,” Malang, 2018.

[17] M. V Pawar and J. Anuradha, “Network Security and Types of Attacks in Network,” *Procedia - Procedia Comput. Sci.*, vol. 48, no. Iccc, pp. 503–506, 2015.

[18] N. Fahriani, P. A. R. Devi, and D. Aditama, “Alternatif Penanganan Jenis Serangan Pencurian Data Pada Jaringan Komputer,” no. November, pp. 24–25, 2017.

[19] J. Ilmiah, I. Komputa, A. A. Zabar, F. Novianto, J. Dipatiukur, and C. Fax, “KEAMANAN HTTP DAN HTTPS BERBASIS WEB MENGGUNAKAN SISTEM OPERASI KALI LINUX Program Studi Teknik Komputer – FTIK Universitas

Komputer Indonesia Jurnal Ilmiah Komputer dan Informatika (KOMPUTA),” vol. 4, no. 2, 2015.

[20] D. Email, A. Ginting, R. R. Isnanto, and I. P. Windasari, “Implementasi Algoritma Kriptografi RSA untuk,” vol. 3, no. 2, pp. 253–258, 2015.

[21] and R. U. Rachmawati and A Budiman, “The cryptanalysis of the Rabin public key algorithm using the Fermat factorization method The cryptanalysis of the Rabin public key algorithm using the Fermat factorization method,” 2019.

[22] A. Khairan, M. Imrona, and I. Ummah, “ANALISIS DAN IMPLEMENTASI KRIPTOGRAFI RSA PADA APLIKASI CHATTING CLIENT-SERVER BASED,” pp. 1–7.

[23] D. M. Khairina, “ANALISIS KEAMANAN SISTEM LOGIN,” vol. 6, no. 2, pp. 64–67, 2011.

UNIVERSITAS MUHAMMADIYAH MALANG
FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK INFORMATIKA
Jl. Raya Tlogomas 246 Malang 65144 Telp. 0341 - 464318 Ext. 247, Fax. 0341 - 460782

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : Ridwan Annas Pryagung
NIM : 201510370311077
Judul TA : IMPLEMENTASI RSA ALGORITHM DAN CYRPTOGRAPHY QUANTUM PADA SISTEM LOGIN

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	2%
2.	Bab 2 – Kajian Pustaka	25 %	16%
3.	Bab 3 – Analisis dan Perancangan	25 %	11%
4.	Bab 4 – Implementasi dan Pengujian	15 %	14%
5.	Bab 5 – Kesimpulan dan Saran	5 %	5%
6.	Makalah Tugas Akhir	20%	7%

Mengetahui,
Dosen Pembimbing

(Sofyan Arifianto, S.Si, M.Kom)

*) Hasil cek plagiarism bisa diisikan oleh salah satu pembimbing